Health Information ARCHITECTURE

Role-Based Access Control (RBAC) Newsletter

Volume 28 – June 2006

Inside this issue:

VHA/IHS RBAC TF Chair
Robert O'Hara, MD
Robert.Ohara@med.va.gov

VHA Deputy Chief Architect
RBAC Project Manager
Steve Wagner
Steve.Wagner@med.va.gov

VHA Security Architect
RBAC Architect
Mike Davis, CISSP
Mike.Davis@med.va.gov

VHA Security Architect
RBAC Architect
Ed Coyne, PhD
Ed.Coyne@med.va.gov

VHA Software Security Architect
Amy Page
Amy.Page@med.va.gov

RBAC Project Lead
Suzanne Webb
Suzanne.Gonzales-Webb@saic.com

~

RBAC and the Next Generation Electronic Commerce Promotion Council of Japan (ECOM) – Lecture Review II

Outline of the "Ninth ECOM Seminar" -Act on the Protection of Personal Information and Attribute Authentication- *On January 27 (Friday), 2006, the monthly ECOM seminar was held at the Kikai Shinko Kaikan Building (Shibakoen, Minato-ku, Tokyo). Under the common theme of "Protection of Personal Information"*

ECOM News No.11 Next Generation Electronic Commerce Promotion Council of Japan

"Act on the Protection of Personal Information and Attribute Authentication"

Mr. Yoji Maeda, Research Director (Security WG, Next Generation Electronic Commerce Promotion Council of Japan)

Under the enforced Act on the Protection of Personal Information and Attribute Authentication, business persons handling personal information are obliged to bear heavier burdens in management measures in handling personal information. There is an expectation on the part of users for the supply of better products and services that meet needs in accordance with personal information and exchange for data.

In the current information network society and for the purpose of controlling access to information, it is necessary to confirm roles and authorities by making use of not only personal authentication, but also personal information. Site administrators, per Mr. Maeda need to handle various kinds of personal information and attribute authentication protection. The Act on the Protection of Personal Information and Attribute Authentication was enforced in April

Upcoming Meetings

- **11th ACM SACMAT 06 Conference**
  June 7-9, 2006
  Lake Tahoe, CA
- **ANSI – Open Forum for Standards Developers**
  June 20-21, 2006
  New York, NY
- **HL7 Educational Summit**
  July 11-13, 2006
  Philadelphia, PA
- **HL7 20th Annual Plenary & Working Group**
  September 10-15, 2006
  Boca Raton, FL
- **ONC (ONCHIT)**
  American Health Information Community Meeting
  October 7, 2006
  Washington, DC 20201
- **ASTM Committees E31 May 2006 Meeting (in conjunction w/TEPR)**
  November 12-14, 2006
  Atlanta, GA

~

RBAC Newsletter Editor
ATTN: Suzanne Webb
RBAC Project Lead
10260 Campus Point MS-B1E
La Jolla, CA 92121

Or e-mail:

Suzanne.Gonzales-Webb@va.gov

2005. With the development of information technology and use of the Internet, more and more personal information is being collected and used. But, at the same time, with the occurrence of large-scale leaks of personal information, cold-calls, nuisance e-mails, etc., the appropriate handling of personal information has become a grave social concern.

Authentication for controlling access to information is classified into personal authentication and attribute authentication. Personal authentication means identity verification based on ID/passwords, IC cards, biometric information and other similar data. Attribute authentication refers to the verification of the accuracy of identity attribute information (i.e. name, address, telephone number, sex, school or company name, title, qualification, preferences, etc.) that is needed to determine whether services will be provided or not. The following methods exist for attribute authentication: the writing of attribute information in public key certificates, the use of attribute certificates in which attribute information is newly written, and management based on databases. If the attribute authentication method based on public key certificates is adopted, attribute information will be made known to the general public. Using this method, attributes and attribute values are shown in certificates, and it will be necessary to reissue public key certificates when attributes and attribute values are changed. It is highly possible to make use of PKI-related software that is commercially available and it is relatively easy to construct these systems.

Per Mr. Maeda, the attribute authentication based on attribute certificates (AC) has the following advantages: the period of validity of attributes can be clearly set and controlled; attributes can be easily administered in a decentralized manner by means of attribute authentication transfers between attribute certificate authorities; the prevention of the falsification of attributes and attribute values is guaranteed by digital signatures. There is a disadvantage however, in that there is a great deal of cost to construct systems when and where standardization and international standardization have not been sufficiently promoted. Attribute authentication based on

~

RBAC Newsletter Editor

ATTN: Suzanne Webb
RBAC Project Lead
10260 Campus Point MS-B1E
La Jolla, CA 92121

Or e-mail:

Suzanne.Gonzales-Webb@va.gov

database management, which includes methods such as the storage of attribute data in databases or directory servers, facilitates the centralized control of the addition of attributes and changes in attribute values. It lacks interoperability because methods for exchanging attributes and attribute values and management methods have not been standardized.

It is now expected that attribute authentication will be necessary to control access to information, but it has not been fully examined in many areas except in medical services and so forth. Mr. Maeda feels that it is necessary to further examine the use of attribute information and interoperability in consideration of the enforced Act on the Protection of Personal Information and Attribute Authentication.

http://www.ecom.jp/en/ecomnews/ecomnews_no11.html#11_4
February 28, 2006

RBAC at INFOSEC

SAIC has been working with the VHA Security Architect to demonstrate various aspects of security services documented in the VHA Architecture Blueprint. The initial phase of the pilot has just completed and several demonstrations from the pilot were running on the convention floor. These demonstrations fall into several categories: delegation, trusted third party authentication, and role based access control.

BEA ran a demo in their booth which showed a demonstration of delegation based loosely on the future My HealtheVet portal. Although a mock up, the important aspect is that the delegation is controlled by centralized policies within the VHA Security Framework.

BEA also ran a SAML interoperability demonstration at their booth. Their demonstration showed how a user can authenticate to a VA resource for authorization to network access (in this example IBM/Tivoli) based on current job tile. Successful authentication generates a SAML token that can be used to automatically

~

RBAC Newsletter Editor

ATTN: Suzanne Webb
RBAC Project Lead
10260 Campus Point MS-B1E
La Jolla, CA 92121

Or e-mail:

Suzanne.Gonzales-Webb@va.gov

authenticate the user to the VHA infrastructure (in this example BEA), where the user roles can be more granular and determine access to functionality within various VHA applications. SAML identity assertions can also be generated within the VHA network, providing us with a nice example of SAML interoperability between IBM and BEA.

Quest software ran a demo of a trusted third party authentication using their VSJ software. This shows a rich client using Active Directory information to authenticate and pass role information into the security framework. The role information can be used by the security framework to make access control decisions.

All of the use cases from the pilot were designed to illustrate possible solutions to expected issues in the future challenge of implementing the future security architecture.

RBAC Taskforce – Update

The next RBAC Taskforce meeting will be held June 7th at 1100 PST/0800 EST/0900 CT. The RBAC Taskforce will continue the discussion regarding the addition of constraints to the current Permission Catalog and Roles. Members will be contacted with a meeting agenda and additional materials in preparation for the meeting.

~

Role-Based Access Control is critically important to the security aspects of the VA and other healthcare organizations. There is a growing management and security demand for RBAC to be implemented in healthcare systems.

RBAC grants rights and permissions to roles rather than individual users. Users then acquire the rights and permissions by being assigned to appropriate roles. By grouping individuals with other individuals who have similar access rights, RBAC can provide significant security management efficiencies. The latest RBAC Documentation additions and prior RBAC Newsletters can be found on the RBAC Website.